Thursday, April 24. 2008

Nagios - Aktiv oder passive Checks?

Nachdem ich jetzt endlich weiss welche Hosts ich monitoren will und welche Dienste ist die Frage auf welchem Wege das stattfinden soll.

Generell gibt es drei "generische" MÃ¶glichkeiten:

Der Nagios-Server selbst fÃ¼hrt selbst Tests aus
Der Nagios-Server "bittet" den entfernten Rechner einen Test auszufÃ¼hren
Ein Test wird ausgefÃ¼hrt und Nagios "nur" das Ergebnis mitgeteilt

Die ersten beiden Methoden sind sogenannte Aktive Checks - Nagios selbst fÃ¼hrt die Checks aus oder stÃ¶ÃŸt einen Task an der den Check ausfÃ¼hrt.

Der letzte Test ist ein sogenannter Passiver Check; Nagios selbst ist nicht fÃ¼r den Test verantwortlich sondern verarbeitet nur das Ergebnis.

Gerade in Netzwerken wo es Firewalls gibt oder Sicherheitsbestimmungen ist die Wahl der Checks durchaus interessant. Nicht alle Checks kann der Nagios-Server selbst machen; ob auf entfernten Rechnern die Festplatte Ã¼berlÃ¤uft zum Beispiel kann er nicht einfach sehen.
Daher gibt es diese zweite Kategorie - fÃ¼r Router oder andere Systeme kann man snmp einsetzen, aber auch den Befehl via ssh auf dem entfernten Rechner auszufÃ¼hren ist eine Option. FÃ¼r Windows-Rechner gibt es auch ein entsprechendes Programm welches auch als Service installiert werden kann.

In allen FÃ¤llen bekommt Nagios vier wichtige Angaben gesagt:

einen Zeitstempel (Epoch)
einen Nagios-internen Befehl
Den Host von dem der Check kommt
Der Status des Dienstes (0 = OK, 1 = Warning, 2= Critical, 3 = Unknown)
Ein freier Text den der Check ausgeben kann

Mit Hilfe des Status hat Nagios seine Aktionen definiert - bei Critical-Meldungen im Melde-Zeitrahmen gibt es zum Beispiel eine Mail an die Beteiligten; wenn der Dienst wieder OK ist, ebenfalls. Es gibt auch die MÃ¶glichkeit dass Dienste eine Zeitlang nicht Ã¼berprÃ¼ft werden - wenn sie fÃ¼r lÃ¤ngere Zeit ausgefallen sind zum Beispiel.

Zu wissen, welche Daten Nagios dringend braucht ist wichtig wenn man eigene Plugins schreibt (weil die Standard-Plugins nicht helfen oder weil man alles fÃ¼r sich anpassen mÃ¶chte); aber auch wenn man passive Checks nutzen will. Bei passiven Checks werden Der Host, der Service, die Statusnummer und der Freitext Ã¼blicherweise mit Hilfe des programms NSCA an den Nagios-Server geleitet. Die Checks mÃ¼ssen natÃ¼rlich definiert sein fÃ¼r den Host, damit die Nachrichten korrekt zugeordnet werden kÃ¶nnen.

Passive Checks haben aber auch einen weiteren Vorteil: Man kann nagios anweisen zu Ã¼berprÃ¼fen wann der letzte passive Check eines Dienstes passiert ist - und wenn diese Zeit zuende ist wird ein aktiver Check durchgefÃ¼hrt. Diesen aktiven Check kann man dann so konfigurieren dass der Dienst sofort auf Critical gesetzt wird. Ich nutze diese Methode gerade um einen Monitor zu Ã¼berwachen - wenn nach 125 Sekunden keine neuen Daten kamen meldet sich nagios und sagt mir dass der Monitor nicht mehr tut. Sehr sinnvoll, besonders abends wenn keiner mehr vor Ort sein mÃ¶chte.

Passive Checks haben aber auch noch einen anderen Vorteil; gerade bei uns. Unsere Netze sind sehr sauber voneinander getrennt - Produktions, Test, Entwicklungsumgebungen, Internet usw. Und unsere Monitoring-Station muss von allen Netzen auch die Daten ja bekommen. Das kÃ¶nnte durchaus zu Problemen mit Firewalls fÃ¼hren.

Was aber unkritisch ist ist wenn die Rechner zum Monitoring hin eine Verbindung aufbauen und nicht andersrum. Daher

sind die passiven Checks sehr angenehm - mit Hilfe von nsca macht der zu Ã¼berprÃ¼fende Rechner auf und nicht der Nagios-Server.

Posted by rince in Tutorials at 20:50

Als ich mich zuletzt mit passiven Checks beschÃ¤ftigt hatte, fehlte an der Stelle der Code, der den Output eines Nagios-Plugins an send_nsca verfÃ¼ttert - send_nsca braucht zum Beispiel den Status auf der Kommandozeile, wÃ¤hrend das Plugin ihn als exit code zurÃ¼ckliefert.

Muss man sich an dieser Stelle immer noch selbst was scripten, oder wird da inzwischen was mitgeliefert was Konfigurationen wie

send_nsca --command="plugin parameters"

ermÃ¶glicht?
Anonymous on Apr 25 2008, 10:11

Es hat sich daran nichts geÃ¤ndert. Allerdings ist das Ziel von passiven Checks ja auch eigentlich nicht, aktive Checks auf anderen Rechnern auszufÃ¼hren (dafÃ¼r gibts check_ssh oder check_nrpe); sondern eigene Scripte oder Tests zu haben und das Egebnis dann an send_nsca zu schicken. Ich habe dafÃ¼r die vorhandenen Test-Scripte einfach erweitert indem ich dort die Exitcodes der Checks abfrage und eine Datei erstelle; pro Test (also Schnittstelle) eine Zeile. Und am Ende rufe ich einmal send_nsca auf um alles auf einmal zu schicken - gerade fÃ¼r die Performance ist dies deutlich besser.
Anonymous on Apr 26 2008, 16:59

Naja, aber fÃ¼r die eigenen Tests Nagios-Plugins verwenden zu kÃ¶nnen wÃ¼rde ich durchaus fÃ¼r ein Feature halten. Zum Beispiel fÃ¼r Hosts, die hinter NAT stehen und die deswegen ihre Ergebnisse nur zum Nagios pushen kÃ¶nnen; dafÃ¼r hÃ¤tte ich gerne eine MÃ¶glichkeit, das nur mit "offiziellem" Nagios-Code hinzubekommen.

Es fehlt wirklich nur der Glue zwischen dem Nagios-Plugin und send_nsca
Anonymous on Apr 26 2008, 19:36